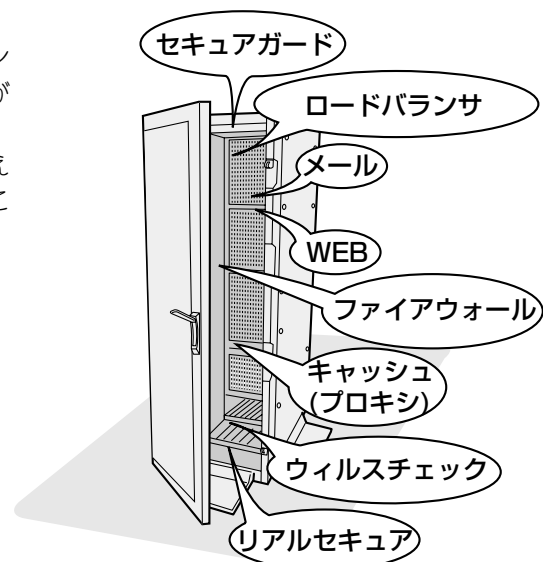
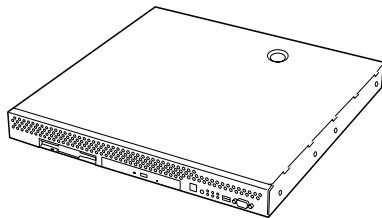
1 InterSec シリーズについて

本製品や添付のソフトウェアの紹介や導入の際に知っておいていただきたい事柄について説明します。

InterSecシリーズとは

「オール・イン・ワン」から「ビルドアップ」へ。
高度なセキュリティ管理により、安全かつ高速なインターネットビジネスを可能にするために生まれたのが「InterSecシリーズ」です。
お使いになる環境や用途に応じて必要となる機能を備えた装置を追加することでシステムをビルドアップすることができます。

1台のラックにそれぞれの機能を持つ装置を搭載(クラスタ構成可能)

InterSecシリーズの主な特長と利点は次のとおりです。

- **省スペース**

  設置スペースを最小限に抑えたコンパクトな筐体を採用。

- **運用性**

  運用を容易にする管理ツール。

- **高い信頼性**

  単体ユニットに閉じた動作環境で単機能を動作させるために、障害発生の影響は個々のユニットに抑えられます。また、絞り込まれた機能のみが動作するため、万一の障害発生時の原因の絞り込みが容易です。

- **高い拡張性**

  専用機として、機能ごとに単体ユニットで動作させているために用途に応じた機能拡張が容易に可能です。また、複数ユニットでクラスタ構成にすることによりシステムを拡張していくことができます。

- **コストパフォーマンスの向上**

  運用目的に最適なチューニングが行えるため、単機能の動作において高い性能を確保できます。また、単機能動作に必要な環境のみ提供できるため、余剰スペックがなく低コスト化が実現されます。

- **管理の容易性**

  環境設定や運用時における管理情報など、単機能が動作するために必要な設定のみです。そのため、導入・運用管理が容易に行えます。

InterSecシリーズには、目的や用途に応じて次のモデルが用意されています。

- **RSシリーズ(リアルセキュア)**

  Internet Security Systems社の不正侵入検知システムである「RealSecure Network Sensor」を搭載した装置です。ネットワークを介した外部からの侵入や攻撃、その他セキュリティ関連のイベントをリアルタイムに監視し、システムやネットワークのアクティビティを分析するセキュリティサービスを提供する装置です。

- **MWシリーズ(メール/WEB)**

  WebやFTPのサービスやインターネットを利用した電子メールの送受信や制御などインターネットで必要となるサービスを提供する装置です。

- **FWシリーズ(ファイアウォール)**

  CheckPoint FireWall-1を搭載し、高度なアクセス制御が可能な、大中規模の企業ネットワーク向けのファイアウォール専用機です。

- **SGシリーズ(ファイアウォール)**

  インターネットと接続した中小規模の企業ネットワークを外部からの不正なアクセスから守るファイアウォール専用機です。

- **LBシリーズ(ロードバランサ)**

  複数台のWebサーバへのトラフィック(要求)を整理し、負荷分散によるレスポンスの向上を目的とした装置です。

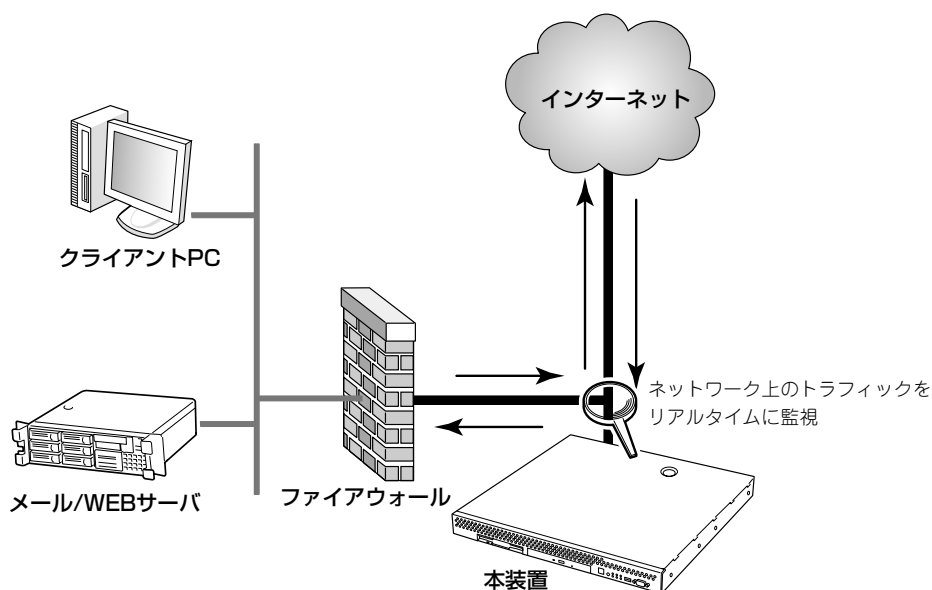
- **CSシリーズ(プロキシ)**

  Webアクセス要求におけるプロキシでのヒット率の向上(Forward Proxy)、Webサーバの負荷軽減・コンテンツ保護(Reverse Proxy)を目的とした装置です。

- **VCシリーズ(ウィルスチェック)**

  インターネット経由で受け渡しされるファイル(電子メール添付のファイルやWeb/FTPでダウンロードしたファイル)から各種ウィルスを検出/除去し、オフィスへのウィルス侵入、外部へのウィルス流出を防ぐことを目的とした装置です。

特長と機能

本製品はInternet Security Systems(ISS)社のRealSecure Network Sensor 7.0をプリインストールした不正侵入検知アプライアンス機器です。
インターネットと接続されたネットワークへの外部からの不正なアクセスを管理者はリアルタイムに把握することができます。

特　長

- 圧倒的なシェアをもつ侵入検知製品の最新版RealSecure Network Sensor 7.0をプリインストールしているので短時間で侵入検知システムが導入できます。
- 1250を超えるプロトコルデコードとシグネチャを有し、膨大な侵入のパターンに対処できます。
- 業界最大でもっとも知名度の高いISS社のセキュリティ研究グループX-Forceの成果を利用して、新たな脅威をスピーディーに製品に反映しています。

  アップデータはX-Press Update(XPU)としてISS社のWebから入手でき、管理コンソールから容易に適用できます。
- プロトコル解析技術との統合により、多くのシグネチャを適用した状態で、100Mbitネットワークを取りこぼしなく監視することが可能です。(標準でHigh Performanceモードを実装)

- 膨大なTCPセッションが同時に発生しても、それを追跡し続けます。ボリュームの大きいWebのトラフィックやその他のセッションベースのトラフィックを処理する際に、比類ない正確性と信頼性を提供します。
- 環境固有の誤検出を減らすため、特定のIP範囲からのイベントに対するフィルタ設定やイベント信頼を行う機能を備えています。
- 類似したイベントがリアルタイムで検出された場合、それらを統合する機能を備えています。より効率的なイベント管理が可能です。
- Network Sensorと管理コンソール間の通信を、強力なRSA暗号(RSA1024-bitに加え、RSA1536-bit)で保護しています。
- オープンソース侵入検知システムSnortのシグネチャのほとんどをインポートすることが可能です。
- 検知イベントに関連したパケットを、一般的なsnifferファイル形式で記録することができます。また、センサーを通過した全トラフィックストリームのキャプチャも可能です。
- 関連製品

  サーバ自身に出入りするパケットやログを監視して侵入を検知するホストベースの侵入検知製品(RealSecure ServerSensor)や、脆弱性検出製品(Internet Scanner)などをラインナップしています。
- ESMPRO

  ESMPRO/ServerAgentを添付しているため、他のExpress5800/InterSec(インターネットアプライアンス)機器と共に統合管理することが可能です。ESMPROは本侵入検知製品の状態管理を行い、GUIにより視覚的に情報を表示します。

機　能

本装置は以下の機能を提供します。

- **侵入検知機能**

  ネットワーク上のパケットを監視、1250以上のプロトコルデコードとシグネチャとの比較により、不正アクセスを検知します。
- **イベント機能**

  不正アクセスが検知されたとき、SNMP、メール、OPSEC、ユーザコマンドなど、様々な手段で通知を行います。イベント発生時のファイアウォール(Firewall-1)との連係機能も有しています。

- **統合管理機能**

GUIにより使用するシグネチャや侵入検知時の動作などを設定することができる管理コンソール製品を添付しています(Windowsマシンにインストール)。複数台のセンサーを一元管理することも可能です。構築するシステム構成に応じて、管理製品をRealSecure Workgroup Manager、RealSecure SiteProtectorの2つから選択できます。

－ RealSecure Workgroup Manager

不正侵入防御システム(RealSecure Network Sensor、RealSecure Server Sensor)の統合管理および、システム規模に応じて最大3階層構造による柔軟な設計が可能です。

－ RealSecure SiteProtector

不正侵入防御システム(RealSecure Network Sensor、RealSecure Server Sensor、RealSecure Desktop Protector)、脆弱性検査ツール(Inetnet Scanner、System Scanner)の統合管理が可能です。

また、Internet ScannerおよびRealSecure SiteProtector Security Fusion Moduleを別途購入頂くことで、脆弱性情報と不正侵入検知(攻撃)情報を相関分析し、ネットワークが持つ既知の脆弱点に対するセキュリティイベントをリアルタイムかつ自動的に監視することが可能です。

- **不正なTCPコネクション遮断機能**

攻撃元マシンが内部ネットワークに対して行った不正アクセスを検知した直後に、ネットワークを監視しているインターフェースからその攻撃元に対してRSKillパケット(TCPのRSTフラグをオンにしたパケット)を送信することでTCPコネクションを遮断し、不正アクセスのシャットアウトが可能です。

添付のディスクについて

本装置にはセットアップや保守・管理の際に使用するCD-ROMやフロッピーディスクが添付されています。ここでは、これらのディスクに格納されているソフトウェアやディスクの用途について説明します。

重要 **添付のフロッピーディスクやCD-ROMは、システムのセットアップが完了した後でも、システムの再セットアップやシステムの保守・管理の際に使用する場合があります。なくさないように大切に保管しておいてください。**

● バックアップCD-ROM

システムのバックアップとなるCD-ROMです。

再セットアップの際は、このCD-ROMと添付の「バックアップ CD-ROM用インストールディスク」を使用してインストールします。詳細は3章を参照してください。

バックアップCD-ROMには、システムのセットアップに必要なソフトウェアや各種モジュールの他にシステムの管理・監視をするための専用のアプリケーション「ESMPRO/ServerAgent」と「エクスプレス通報サービス」が格納されています。システムに備わったRAS機能を十分に発揮させるためにぜひお使いください。ESMPRO/ServerAgentの詳細な説明はバックアップCD-ROM内のオンラインドキュメントをご覧ください。エクスプレス通報サービスを使用するには別途契約が必要です。お買い求めの販売店または保守サービス会社にお問い合わせください。

● RealSecureパッケージCD-ROM

－ 管理ソフトウェア（SiteProtector、WorkgroupManagerインストールディスク）

本製品の管理ソフトウェアのインストールディスク(Windows版)です。本製品の設定や本製品が検出した不正アクセスをグラフィカルに表示します。

2種類の管理ソフトウェアがあります。どちらか一方の管理ソフトウェアを管理PCにインストールして使用します。

－ データベースソフト

管理ソフトウェアで使用するデータベースエンジンです。

SiteProtectorの場合は、SQLServerが必須です。

Workgroup Managerの場合は、SQLServerを使用することを推奨します（ただし、MSDE2000を使用することができます）。

この2つのソフトウェアには修正パッチ(同CD-ROMに格納されています)を適用する必要があります。使用する前に必ずパッチを適用してください。

－ 管理ソフトウェアのパッチ・アップデート

日本語化するためのパッチや、初期出荷時で最新版のセキュリティアップデートが含まれています。

－ 各種製品マニュアル

管理ソフトウェアおよびNetwork Sensor関連のマニュアルです。詳細について知りたいときに活用してください。

- **保守・管理ツールCD-ROM**

  本体およびシステムの保守・管理の際に使用するCD-ROMです。

  このCD-ROMには次のようなソフトウェアが格納されています。

  − 保守・管理ツール

    再セットアップの際に装置の維持・管理を行うためのユーティリティを格納するためのパーティション(保守パーティション)を作成したり、システム診断やオフライン保守ユーティリティなどの保守ツールを起動したりするときに使用します。詳細は4章を参照してください。

  − MWA

    システムが立ち上がらないようなときに、リモート(LAN接続またはRS-232Cケーブルによるダイレクト接続)で管理PCから本装置を管理する時に使用するソフトウェアです。詳細は4章を参照してください。

  − ESMPRO/ServerManager

    ESMPRO/ServerAgentがインストールされたコンピュータを管理します。詳細は保守・管理ツールCD-ROM内のオンラインドキュメントを参照してください。

- **バックアップCD-ROM用インストールディスク(フロッピーディスク)**

  システムの再インストールの際に使用します。